

Computing Split Maximal Toral Subalgebras of Lie Algebras over Fields of Small Characteristic

Dan Roozemon, University of Sydney

April 25, 2012

Abstract

Important subalgebras of a Lie algebra of an algebraic group are its toral subalgebras, or equivalently (over fields of characteristic 0) its Cartan subalgebras. Of great importance among these are ones that are split: their action on the Lie algebra splits completely over the field of definition. While algorithms to compute split maximal toral subalgebras exist and have been implemented [Ryb07, CM09], these algorithms fail when the Lie algebra is defined over a field of characteristic 2 or 3.

We present heuristic algorithms that, given a reductive Lie algebra L over a finite field of characteristic 2 or 3, find a split maximal toral subalgebra of L . Together with earlier work [CR09] these algorithms are very useful for the recognition of reductive Lie algebras over such fields.

1 Introduction

For computational problems regarding a split reductive algebraic group G defined over a field \mathbb{F} , it is often useful to calculate within its Lie algebra L over \mathbb{F} . For instance, the conjugacy question for two split maximal tori in G can often be translated to a conjugacy question for two split toral subalgebras of L . A *maximal toral subalgebra* H of L is a commutative subalgebra consisting of semisimple elements (recall that an element $x \in L$ is called semisimple if it is contained in the p -subalgebra generated by x^p), and it is maximal (with respect to inclusion) among subalgebras of L with these properties. For such a subalgebra we have that multiplication (in L) by each of its elements is semisimple, i.e., each of its elements has a diagonal form with respect to a suitable basis over a large enough extension field of \mathbb{F} . A maximal toral subalgebra H is called *split* (or \mathbb{F} -*split*) if, for every $h \in H$, left multiplication by h , denoted ad_h , has a diagonal form with respect to a suitable basis over \mathbb{F} . Such a subalgebra is the Lie algebra of a split maximal torus in G . Recall that \hat{H} is called a *Cartan subalgebra* of L if \hat{H} is nilpotent and $N_L(\hat{H}) = \hat{H}$. Maximal toral subalgebras and Cartan subalgebras are closely related: if H is a maximal toral subalgebra of L , then $C_L(H)$ is a Cartan subalgebra of L [Hum67, Proposition 15.1].

In the case that \mathbb{F} is not of characteristic 2 or 3 a Las Vegas algorithm exists to compute split maximal toral subalgebras, due to Cohen and Murray [CM09, Lemma 5.7]. Independently, Ryba developed a Las Vegas algorithm for computing split Cartan subalgebras [Ryb07]. Unfortunately, Ryba also excludes characteristic 2 and, if the Lie algebra is of type A_2 or G_2 , characteristic 3. It is, however, claimed that the algorithm may work in some cases in characteristic 2, but not in all cases (cf. [Ryb07, Section 9.3]).

In this paper we present heuristic algorithms that, given a reductive Lie algebra L over a finite field of characteristic 2 or 3, find a split maximal toral subalgebra of L . We present separate

algorithms for the two characteristics. Each of these algorithms is Las Vegas: it either returns a subalgebra H of the correct form (with nonzero probability), or it returns **fail**. The algorithm for the characteristic 2 case has been described before in the author's PhD thesis [Roo10, Chapter 3].

The remainder of this paper

The remainder of this section sets the theoretical framework we need to describe the algorithms. In Section 2 we investigate a particular Lie algebra and a split maximal toral subalgebra that is not contained in a split toral subalgebra of maximal dimension. In Section 3 we study the occurrence (or lack thereof) of regular semisimple elements in Lie algebras over fields of characteristic 2, showing that the Las Vegas algorithm by Cohen and Murray cannot easily be applied in those cases. In Section 4 we describe a heuristic algorithm to find split maximal toral subalgebras in the characteristic 3 case, and in Section 5 we describe such an algorithm for the characteristic 2 case. Finally, in Section 6 we comment on the implementation and performance of these algorithms.

Root data

Our treatment of Lie algebras and the corresponding algebraic groups rests on the theory developed mainly by Chevalley and available in the excellent books by Borel [Bor91], Humphreys [Hum75], and Springer [Spr98]. Our set-up is as in [CR09], a publication we will repeatedly refer to because of the extensive analysis it contains on the structure of reductive Lie algebras over fields of small characteristic. We refer to [CR09] for more details on our set-up and restrict ourselves to the essential notions here.

Split reductive algebraic groups are determined by their fields of definition and their root data [Spr98, Theorem 9.4.3]. Throughout this paper we let $R = (X, \Phi, Y, \Phi^\vee)$ be a *root datum* of rank n . This means X and Y are dual free \mathbb{Z} -modules of dimension n with a bilinear pairing $\langle \cdot, \cdot \rangle : X \times Y \rightarrow \mathbb{Z}$ such that the induced map $X \rightarrow \text{Hom}(Y, \mathbb{Z})$ is an isomorphism (and then so is the induced map $Y \rightarrow \text{Hom}(X, \mathbb{Z})$), Φ is a finite subset of X and Φ^\vee a finite subset of Y , and called the *roots* and *coroots*, respectively, and there is a one-to-one correspondence $^\vee : \Phi \rightarrow \Phi^\vee$ such that $\langle \alpha, \alpha^\vee \rangle = 2$ for all $\alpha \in \Phi$. Both the roots Φ and the coroots Φ^\vee should form a root system in the traditional sense. The irreducible root systems are well-known, and described in Cartan's notation A_n ($n \geq 1$), B_n ($n \geq 2$), C_n ($n \geq 3$), D_n ($n \geq 4$), E_n ($n \in \{6, 7, 8\}$), F_4 , G_2 .

A *weight* is a vector w in the Euclidian space $X \otimes \mathbb{R}$ such that $\langle w, \alpha^\vee \rangle \in \mathbb{Z}$ for all $\alpha \in \Phi$. These weights form a weight lattice, and the *fundamental group* is defined to be the quotient of this weight lattice by the root lattice $\mathbb{Z}\Phi$. The subgroups of this fundamental group parametrize the possible semisimple root data with a given root system Φ via the quotient $X/\mathbb{Z}\Phi$. For sake of completeness we remark that the fundamental group is $\mathbb{Z}/(n+1)\mathbb{Z}$ for A_n ; $\mathbb{Z}/2\mathbb{Z}$ for B_n and C_n ; $\mathbb{Z}/4\mathbb{Z}$ for D_n if n is odd, $\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}$ for D_n if n is even; $\mathbb{Z}/3\mathbb{Z}$ for E_6 ; $\mathbb{Z}/2\mathbb{Z}$ for E_7 ; and it is trivial for E_8 , F_4 , and G_2 .

We use this observation to define the *isogeny type* of a root datum. If $X/\mathbb{Z}\Phi$ is the trivial group, R is said to be of *adjoint* isogeny type; if on the other hand $X/\mathbb{Z}\Phi$ is the full fundamental group, R is said to be of *simply connected* isogeny type. If neither of these is the case, R is said to be of *intermediate* isogeny type. Note that the last case only occurs for root systems of type A_n and D_n .

We denote an adjoint root datum whose root system is of type X_n by X_n^{ad} , and its simply connected variant by X_n^{SC} . Intermediate root data of type A_n will be denoted by $A_n^{(k)}$, where $k|n+1$; intermediate root data of type D_n will be denoted by $D_n^{(1)}$ if n is odd, and by $D_n^{(1)}$, $D_n^{(n-1)}$, and $D_n^{(n)}$ if n is even.

Example 1. There are two root data of type A_1 , namely A_1^{ad} and A_1^{SC} . In both cases, $X = Y = \mathbb{Z}$; we may take $e_1 = (1)$ to be a basis of X and $f_1 = (1)$ a basis of Y . For A_1^{ad} , the roots are taken to be $\alpha = (1)$, $-\alpha = (-1)$, the coroots $\alpha^\vee = (2)$, $-\alpha^\vee = (-2)$, and the pairing between X and Y is simply multiplication, so that $\langle \alpha, f_1 \rangle = 1$ and $\langle e_1, \alpha^\vee \rangle = 2$.

Conversely, for A_1^{SC} , the roots are taken to be $\alpha = (2)$, $-\alpha = (-2)$, the coroots $\alpha^\vee = (1)$, $-\alpha^\vee = (-1)$, and the pairing again is multiplication, so that $\langle \alpha, f_1 \rangle = 2$ and $\langle e_1, \alpha^\vee \rangle = 1$.

Chevalley Lie algebras

Given a root datum R we consider the free \mathbb{Z} -module

$$L_{\mathbb{Z}}(R) = Y \oplus \bigoplus_{\alpha \in \Phi} \mathbb{Z}X_{\alpha},$$

where the X_{α} are formal basis elements. The rank of $L_{\mathbb{Z}}(R)$ is $n + |\Phi|$. We denote by $[\cdot, \cdot]$ the alternating bilinear map $L_{\mathbb{Z}}(R) \times L_{\mathbb{Z}}(R) \rightarrow L_{\mathbb{Z}}(R)$ determined by the following rules:

$$\begin{aligned} \text{For } y, z \in Y : \quad [y, z] &= 0, & (\text{CBZ1}) \\ \text{For } y \in Y, \alpha \in \Phi : \quad [X_{\alpha}, y] &= \langle \alpha, y \rangle X_{\alpha}, & (\text{CBZ2}) \\ \text{For } \alpha \in \Phi : \quad [X_{-\alpha}, X_{\alpha}] &= \alpha^\vee, & (\text{CBZ3}) \\ \text{For } \alpha, \beta \in \Phi, \alpha \neq \pm\beta : \quad [X_{\alpha}, X_{\beta}] &= \begin{cases} N_{\alpha, \beta} X_{\alpha+\beta} & \text{if } \alpha + \beta \in \Phi, \\ 0 & \text{otherwise.} \end{cases} & (\text{CBZ4}) \end{aligned}$$

The $N_{\alpha, \beta}$ are integral structure constants chosen to be $\pm(p_{\alpha, \beta} + 1)$, where $p_{\alpha, \beta}$ is the biggest number such that $\alpha - p_{\alpha, \beta}\beta$ is a root and the signs are chosen (once and for all) so as to satisfy the Jacobi identity. It is easily verified that $N_{\alpha, \beta} = -N_{-\alpha, -\beta}$ and it is a well-known result (see for example [Car72, Proposition 4.4.2]) that such a product exists. $L_{\mathbb{Z}}(R)$ is called a *Chevalley Lie algebra*.

For any field \mathbb{F} we define $L_{\mathbb{F}}(R)$ to be the Lie algebra $L_{\mathbb{Z}}(R) \otimes \mathbb{F}$.

Example 2. Corresponding to the two root data of type A_1 described in Example 1 there exist two Chevalley Lie algebras of type A_1 . Both are 3-dimensional and have formal basis elements X_{α} , $X_{-\alpha}$, and h , but their multiplication differs.

The multiplication for the Lie algebra of type A_1^{ad} is determined by $[X_{\alpha}, X_{-\alpha}] = -2h$, $[X_{\alpha}, h] = X_{\alpha}$, and $[X_{-\alpha}, h] = -X_{-\alpha}$ (observe that the multiplication on all other algebra elements follows from bilinearity and anti-symmetry). On the other hand, for A_1^{SC} we have $[X_{\alpha}, X_{-\alpha}] = -h$, $[X_{\alpha}, h] = 2X_{\alpha}$, and $[X_{-\alpha}, h] = -2X_{-\alpha}$.

It is easy to see that $L_{\mathbb{F}}(A_1^{\text{ad}})$ and $L_{\mathbb{F}}(A_1^{\text{SC}})$ are isomorphic unless $\text{char}(\mathbb{F}) = 2$.

A basis of $L_{\mathbb{Z}}(R)$ that consists of a basis of Y and the formal elements X_{α} and satisfies (CBZ1)–(CBZ4) is called a *Chevalley basis* of the Lie algebra $L_{\mathbb{Z}}(R)$ with respect to the split Cartan subalgebra Y and the root datum R . If no confusion is imminent we just call this a *Chevalley basis* of $L_{\mathbb{Z}}(R)$.

The interest in Chevalley Lie algebras comes from the following result.

Theorem 3 (Chevalley [Che58]). *Suppose that L is the Lie algebra of a split semisimple algebraic group G over \mathbb{F} with root datum $R = (X, \Phi, Y, \Phi^\vee)$. Then $L \cong L_{\mathbb{F}}(R)$, and if G is simple then R is irreducible.*

In light of this theorem, we will view all Lie algebras as Chevalley Lie algebras in the remainder of this paper. Moreover, we will only consider Chevalley Lie algebras with an irreducible root datum, as the algorithms presented easily generalise to the case of an arbitrary root datum.

We assume Lie algebras to be given as a vector space together with a list of structure constants that define the products of vectors, i.e., we are given a field \mathbb{F} , a d -dimensional vector space V over \mathbb{F} with basis b_1, \dots, b_d , and structure constants c_{ijk} that are understood to mean

$$[b_i, b_j] = \sum_{k=1}^d c_{ijk} b_k.$$

Example 4. We consider the Lie algebra for A_1^{ad} defined in Example 2. If we take the basis elements to be $b_1 = X_\alpha$, $b_2 = X_{-\alpha}$, and $b_3 = h$, the only nonzero c_{ijk} are: $c_{123} = -2$, $c_{131} = 1$, $c_{213} = 2$, $c_{232} = -1$, $c_{311} = -1$, and $c_{322} = 1$.

This is the standard way of representing a finite dimensional Lie algebra on a computer (see [dG00, Section 1.5]). In general, of course, the basis we are given is arbitrary and not of a particularly nice form such as a Chevalley basis. In fact, when a Chevalley basis is known a split maximal toral subalgebra is easily recovered: it simply is Y .

Root spaces

Let $R = (X, \Phi, Y, \Phi^\vee)$ be a root datum, fix a basis $\{y_1, \dots, y_n\}$ of Y , let \mathbb{F} be a field, $L = L_{\mathbb{F}}(R)$ the Lie algebra of type R over \mathbb{F} , and let $H = Y \otimes \mathbb{F}$ and $h_i = y_i \otimes 1_{\mathbb{F}}$. We call H the *standard split maximal toral subalgebra* of L . We define a *root of H on L* to be the function

$$\bar{\alpha} : H \rightarrow \mathbb{Z}, h \mapsto \sum_{i=1}^n \langle \alpha, y_i \rangle t_i, \text{ where } h = \sum_{i=1}^n y_i \otimes t_i = \sum_{i=1}^n t_i h_i,$$

where n is the rank of R . Note that $\bar{\alpha}$ actually maps into \mathbb{F} , but by construction the image actually consists of integers (cf. Equations (CBZ1) – (CBZ4)). Furthermore, we define the *root space corresponding to $\bar{\alpha}$* to be

$$L_{\bar{\alpha}} = \bigcap_{i=1}^n \text{Ker}(\text{ad}_{h_i} - \bar{\alpha}(h_i)).$$

Example 5. We consider Lie algebras with root data A_2^{ad} and A_2^{SC} over a number of different fields. We denote the roots by $\pm\alpha_1, \pm\alpha_2, \pm(\alpha_1 + \alpha_2)$.

First, suppose $\mathbb{F} = \mathbb{Q}$. In this case, for both A_2^{ad} and A_2^{SC} , all L_{α} are 1-dimensional and distinct. For example, $L_{\alpha_2} = \mathbb{Q}X_{\alpha_2}$.

Second, suppose \mathbb{F} is a field of characteristic 2. Then, for both A_2^{ad} and A_2^{SC} , all L_{α} are 2-dimensional. For example, $L_{\alpha_1} = L_{-\alpha_1} = \mathbb{F}X_{\alpha_1} + \mathbb{F}X_{-\alpha_1}$.

Finally, suppose \mathbb{F} is a field of characteristic 3. Recall from Equation (CBZ2) that the action of H on L (in particular on the X_{α}) depends on the isogeny type of the root datum, so that the root spaces may differ between A_2^{ad} and A_2^{SC} . In this case they indeed do. For A_2^{ad} , all L_{α} are 1-dimensional and distinct. However, for A_2^{SC} , we have

$$\begin{aligned} L_{\alpha_1} &= L_{\alpha_2} = L_{-\alpha_1-\alpha_2} = \mathbb{F}X_{\alpha_1} + \mathbb{F}X_{\alpha_2} + \mathbb{F}X_{-\alpha_1-\alpha_2}, \text{ and} \\ L_{-\alpha_1} &= L_{-\alpha_2} = L_{\alpha_1+\alpha_2} = \mathbb{F}X_{-\alpha_1} + \mathbb{F}X_{-\alpha_2} + \mathbb{F}X_{\alpha_1+\alpha_2}. \end{aligned}$$

2 A characteristic 2 curiosity

For the development of a recursive algorithm for finding split maximal toral subalgebras it would be very helpful to know in advance that every split toral subalgebra is contained in a split toral subalgebra that is maximal among all (not necessarily split) toral subalgebras. The algorithm by Cohen and Murray relies on a similar (but weaker) assertion (cf. [CM09, Proposition 5.8]). This is, however, not in general true in characteristic 2, as we will show in the following example.

We consider the Chevalley Lie algebra L of type C_4^{SC} over $\text{GF}(2)$, with root datum $R = (X, \Phi, Y, \Phi^\vee)$ and Chevalley basis elements $\{X_\alpha, h_i \mid \alpha \in \Phi, i \in \{1, \dots, 4\}\}$. Furthermore, we denote the simple roots of Φ by $\alpha_1, \dots, \alpha_4$, where α_1, α_2 , and α_3 are short roots, and α_4 is long. Its non-simple positive roots are then

$$\begin{aligned} \alpha_5 &= (1, 1, 0, 0), \alpha_6 = (0, 1, 1, 0), \alpha_7 = (0, 0, 1, 1), \alpha_8 = (1, 1, 1, 0), \\ \alpha_9 &= (0, 1, 1, 1), \alpha_{10} = (0, 0, 2, 1), \alpha_{11} = (1, 1, 1, 1), \alpha_{12} = (0, 1, 2, 1), \\ \alpha_{13} &= (1, 1, 2, 1), \alpha_{14} = (0, 2, 2, 1), \alpha_{15} = (1, 2, 2, 1), \alpha_{16} = (2, 2, 2, 1), \end{aligned}$$

where (c_1, c_2, c_3, c_4) denotes $c_1\alpha_1 + c_2\alpha_2 + c_3\alpha_3 + c_4\alpha_4$, and the negative roots are defined accordingly. Now let

$$\begin{aligned} y_1 &= h_1 + h_3 \in Z(L), \\ y_2 &= h_1 + X_{\alpha_{12}} + X_{-\alpha_8}, \\ y_3 &= h_2 + X_{\alpha_3} + X_{-\alpha_3} + X_{\alpha_{15}} + X_{-\alpha_{15}}, \end{aligned}$$

and $H = \langle y_1, y_2, y_3 \rangle_L$.

Proposition 6. *The subalgebra H is a 3-dimensional split toral subalgebra of L . There, however, does not exist a split toral subalgebra H' of L of dimension 4 such that $H \subseteq H'$.*

Proof It is straightforward to verify that H is a split toral subalgebra of L : on diagonalization of H in the adjoint representation we obtain 3 eigenspaces of dimension 8 (corresponding to roots $(0, 1, 0)$, $(0, 0, 1)$, and $(0, 1, 1)$) and an eigenspace L_0 of dimension 12 (corresponding to the root $(0, 0, 0)$ and H itself).

Now suppose there exists a split toral subalgebra H' of dimension 4 containing H . This would imply the existence of a $y \in H'$ such that $y \notin H$ and $[y, H] = 0$. Furthermore, by the structure of the root spaces of L (cf. [CR09, Proposition 3]), diagonalization with respect to H' would give 6 eigenspaces of dimension 4, and one eigenspace L'_0 of dimension 12 (where $H' \subseteq L'_0$). This means in particular that $L_0 = L'_0$ and that y should have a unique eigenvalue on L_0 . Since $[y, H] = 0$ and $H \subseteq L_0$, the eigenvalue of y on L_0 must be 0, and thus $y \in C_{H'}(L_0)$, implying $y \in C_L(L_0)$.

However, $C_L(L_0)$ is 4-dimensional and $y_1, y_2, y_3 \in C_L(L_0)$, so that (modulo linear combinations of y_1, y_2, y_3 , and up to scalar multiples) there is only one choice for y :

$$y = h_3 + h_4 + X_{\alpha_3} + X_{\alpha_9} + X_{\alpha_{12}} + X_{-\alpha_3} + X_{-\alpha_5}.$$

Because the characteristic polynomial of ad_y is equal to $x^{16}(x+1)^4(x^2+x+1)^8$, we see that y is not split, and that therefore H' is not a split toral subalgebra: a contradiction. \square

This demonstrates that H is an example of a split toral subalgebra that is not contained in a split toral subalgebra that is maximal among all toral subalgebras.

3 Regular semisimple elements

In [CM09] Cohen and Murray describe an algorithm for Lang's theorem, which needs an algorithm to find split maximal toral subalgebras of Lie algebras. Although they do not claim their algorithm is valid in the characteristic 2 case, some propositions are. We shall first introduce the concept of regular semisimple elements in order to expose some of the difficulties in characteristic 2.

An element x of a Lie algebra L is called *regular semisimple* if its centralizer $C_L(x)$ is a maximal toral subalgebra. We denote the set of regular semisimple elements of L by L_{rss} . Moreover, if L is the Lie algebra of a group of Lie type with root datum R we let $L_{\text{rss},w}$ be the set of elements $x \in L_{\text{rss}}$ for which there exists a $g \in G$ such that $C_L(x) = H_0^g$ and $g^F g^{-1} \in T_0 \dot{w}$, where T_0 is the standard split maximal torus, $H_0 = \text{Lie}(T_0)$ the corresponding split maximal toral subalgebra, F denotes the Frobenius automorphism of the field, and \dot{w} denotes a lift of the Weyl group element w . In this section we are primarily interested in split toral subalgebras, hence in $L_{\text{rss},\text{id}}$.

The time analysis in [CM09] uses the fact that a significant fraction of the elements in the Lie algebra is regular semisimple. In the following proposition we show that this is not always true over fields of characteristic 2.

Proposition 7. *Let \mathbb{F} be a field of characteristic 2, let R be a root datum of type A_1^{SC} , B_2^{SC} , or C_n^{SC} (where $n \geq 3$), and let L be the Lie algebra of type R over \mathbb{F} . There exist no regular semisimple elements in L .*

Proof We refer to the analysis of these Lie algebras detailed in [CR09, Proposition 3, Table 1], where it is shown that in the cases mentioned some of the root spaces are contained in the 0-eigenspace of a split maximal toral subalgebra. This in particular implies that if H is a split maximal toral subalgebra of L then $H \subsetneq C_L(H)$. So suppose $x \in L_{\text{rss},\text{id}}$, so that $C_L(x) = H$, for some split maximal toral subalgebra H of L . However, $x \in H$ since $x \in C_L(x)$, so that $C_L(x) \supseteq C_L(H) \supsetneq H$, a contradiction. \square

This shows that in some cases in characteristic 2 there is a complete absence of regular semisimple elements. A straightforward counting exercise [Roo10, Section 3.2] shows that in other cases in characteristic 2 regular semisimple elements are scarce as well, and even over small fields of odd characteristic the number of regular semisimple elements may be quite small.

4 The characteristic 3 case

We first remark that the troublesome characteristic 3 cases that Ryba [Ryb07] excludes are precisely those cases discussed in [CR09, Section 2]: the Lie algebras whose root datum is either A_2^{SC} or G_2 . The problems that arise here may be remedied relatively easily, following the observation that even though some root spaces have dimension 3 (rather than the more desirable dimension 1), the product of random elements of two opposite 3-dimensional eigenspaces is often a split semisimple element.

The algorithm is made explicit as Algorithm 8: we recursively find a semisimple element h , find two opposite eigenspaces S^+ and S^- of h , and consider random elements $s^+ \in S^+$ and $s^- \in S^-$. If $h' = [s^+, s^-]$ pulls back to a split semisimple element of L , we add h' to the subalgebra H being constructed, and continue in $C_M(h')/\langle h' \rangle_M$. Throughout the algorithm, H is a split toral subalgebra of L , M is a Lie algebra being searched for new split semisimple elements, and φ is the pullback map from M to L . Note that the image of φ is not uniquely determined, but it is determined up to addition with elements of H .

SPLITMAXIMALTORALSUBALGEBRA3

in: A Lie algebra L over a finite field \mathbb{F} of characteristic 3,
out: A split maximal toral subalgebra H of L .
begin
1 **let** $M = L$, $H = 0$, $\varphi = \text{id}$,
2 **while** $M \neq 0$ **do**
 / Base case */*
3 **if** $[M, M] = 0$ **and** $\varphi(M)$ is split semisimple in L **then**
4 **let** $H = H \cup \varphi(M)$,
5 **return** H .
6 **end if**
 / Try to find a new element of H */*
7 **let** ad_M be the adjoint representation of M ,
8 **let** h be a random non-zero semisimple element of M ,
9 **for each** pair of eigenvalues $(v, -v)$ of $\text{ad}_M(h)$ **do**
10 **let** $s^+ \in M$ be a random element of the v -eigenspace of $\text{ad}_M(h)$,
11 **let** $s^- \in M$ be a random element of the $-v$ -eigenspace of $\text{ad}_M(h)$,
12 **let** $h' = [s^+, s^-]$,
13 **if** $h'_L = \varphi(h')$ is a split semisimple element of L **then**
14 **let** $H = H \cup h'_L$,
15 **let** $M, \varphi_M = C_M(h') / \langle h' \rangle_M$,
16 **let** $\varphi : M \rightarrow L, \varphi_M \circ \varphi$ the new pullback of M to L ,
17 **break for**.
18 **end if**.
19 **end for**.
20 **end while**,
21 **return** H .
end

Algorithm 8: Finding a split maximal toral subalgebra in char. 3

In Section 6 we present timings for Algorithm 8 applied to Chevalley Lie algebras in characteristic 3. We remark that in our experience this algorithm is applicable to and yields correct results for all Chevalley Lie algebras over finite fields of any odd characteristic.

5 The characteristic 2 case

Proposition 7 indicates that the approach for finding split maximal toral subalgebras described by Cohen and Murray [CM09, Section 5] will not in general work in the cases covered by the proposition: there simply do not exist any regular semisimple elements in the Lie algebra. Moreover, their algorithm relies on the fact that root spaces are 1-dimensional, something that is not true over characteristic 2 [CR09, Proposition 3].

Ryba explicitly notes [Ryb07, Section 9] that the algorithm he describes is not easily extended to work over fields of characteristic 2, largely because of similar problems. Finally, the counterexample presented in Section 2 suggests that algorithms for finding split maximal toral subalgebras run the risk of descending into a split toral subalgebra that is not in a split maximal toral subalgebra.

In this section we describe a heuristic Las Vegas type algorithm for finding split maximal toral subalgebras in characteristic 2. Unfortunately, we have no bound on the probability that it completes successfully, and therefore no estimate of the runtime. However, we do provide the intuition behind the design of the algorithm (in the remainder of this section) and we show that the implementation is successful (we give timings in Section 6).

For the remainder of this section we let L be the Lie algebra of a split simple algebraic group defined over a finite field \mathbb{F} of characteristic 2, and we assume L to be given as a structure constant algebra. The goal of the algorithm described is to find a split maximal toral subalgebra H of L .

The general principle is given in Algorithm 9. This algorithm repeatedly tries to find a split semisimple element $h' \in M$ (initially $M = L$), and then recursively continues the search in $C_M(h')/\langle h' \rangle_M$. It attempts to find such split semisimple elements by taking a random non-zero semisimple element h , and producing a random split semisimple element using suitable eigenspaces of h . The latter process is described in Algorithm 10.

In order to clarify Algorithm 10 we let R be an irreducible root datum, \mathbb{F} a field of characteristic 2, and L the Lie algebra of type $R = (X, \Phi, Y, \Phi^\vee)$ over \mathbb{F} . Recall the definition of root spaces L_α from Section 1. Observe first of all that, since $\text{char}(\mathbb{F}) = 2$, the root spaces L_α and $L_{-\alpha}$ coincide for all $\alpha \in \Phi$. This implies that $\alpha^\vee \in [L_\alpha, L_\alpha]$, prompting us to consider $[S, S]$ in line 4 of Algorithm 10.

We justify the choices for the various other cases in this algorithm using the data in Table 1. In the first column that table contains the root data R that are proved to have multidimensional root spaces over fields of characteristic 2 (cf. [CR09, Proposition 3]). The hook symbols in the first column indicate a case spread over multiple rows, e.g., the 5th and 6th row both concern the case B_2^{ad} . The second column labeled “Mult” contains the dimensions and multiplicities of each of these root spaces in the same notation used in [CR09], i.e., d^k signifies k distinct eigenspaces of dimension d and such a \mathbf{d}^k printed in boldface indicates an eigenspace that occurs with eigenvalue 0.

To clarify the other columns we let V be one of the eigenspaces mentioned (e.g., for the eighth line of the table $L = B_n^{\text{ad}}(\mathbb{F})$ and V is one of the 4-dimensional (long) root spaces). Then we let $S = \langle V \rangle_L$ be the subalgebra generated by V and $I = (V)_L$ the ideal generated by V . Now the third column contains the dimension of S , the fourth column the dimension of $[S, S]$ and the fifth the dimension of $[S, S] \cap H$. The sixth column contains the dimension of I , or “ L ” if $I = L$, or


```

SPLITMAXIMALTORALSUBALGEBRA2
in:      A Lie algebra  $L$  over a finite field  $\mathbb{F}$  of characteristic 2,
out:    A split maximal toral subalgebra  $H$  of  $L$ .
begin
1  let  $d = \dim(C_L(\hat{H}))$  where  $\hat{H}$  is some Cartan subalgebra of  $L$ ,
2  let  $M = L$ ,  $H = 0$ ,  $\varphi = \text{id}$ ,
3  while  $M \neq 0$  and  $\dim(H) < d$  do
4    if  $\dim(Z(M)) > 0$  then
      /* Take out the center */
5    if  $\varphi(Z(M))$  is split semisimple then let  $H = H \cup \varphi(Z(M))$ .
6    let  $M, \varphi_M = M/Z(M)$ ,
7    let  $\varphi : M \rightarrow L, \varphi_M \circ \varphi$ .
8  else
      /* Try to find a new element of  $H$  */
9    let  $h$  be a random non-zero semisimple element of  $M$ ,
10   if  $\varphi(h)$  is split semisimple in  $L$  then
11     let  $h' = h$ .
12   else
      /* Use this  $h$  as input for FINDSPLITSEMISIMPLEELT */
13   for each eigenvalue  $v$  of  $h$  do
14     let  $V$  be the  $v$ -eigenspace of  $h$ ,
15     let  $h' = \text{FINDSPLITSEMISIMPLEELT}(V, M, L, \varphi)$ ,
16     if  $h' \neq \text{fail}$  then break.
17   end for,
18   end if,
19   if  $h' \neq \text{fail}$  then
20     let  $H = H \cup h'$ ,
21     let  $M, \varphi_M = C_M(h')/\langle h' \rangle_M$ ,
22     let  $\varphi : M \rightarrow L, \varphi_M \circ \varphi$ .
23   end if.
24 end if.
25 end while.
end

```

Algorithm 9: Finding a split maximal toral subalgebra in char. 2

FINDSPLITSEMISIMPLEELT

in: An eigenspace V of a semisimple element of the Lie algebra $M \subseteq L$,
and the natural pullback map $\varphi : M \rightarrow L$.

out: A split semisimple element $h \in M$, or **fail**.

begin

- 1 **let** $S = \langle V \rangle_M$ be the subalgebra of M generated by V ,
- 2 **let** $I = (V)_M$ be the ideal of M generated by V ,
- 3 **if** $\dim([S, S]) = 1$ **then**
/ Case (A) */*
- 4 **let** $h' \in [S, S]$ be such that $[S, S] = \langle h' \rangle_{\mathbb{F}}$.
- 5 **else if** $[I, I] = I$ **and** $\dim([S, S]) \in \{2, 3\}$ **then**
/ Case (B) */*
- 6 **let** h' be a random non-zero element of $[S, S]$.
- 7 **else if** $\dim(I) \neq 0$ **and** $\dim(I)$ is even **and** $\dim([I, I]) = 0$
and $\dim([S, S]) = 0$ **then**
/ Case (C) */*
- 8 **find** an $h' \in M$ such that $[h', e] = e$ for all $e \in I$.
- 9 **else if** $\dim(S) = 6$ **and** $[I, I] = S$ **and** $\dim([S, S]) = 2$ **then**
/ Case (D) */*
- 10 **let** h' be a random non-zero element of $[S, S]$.
- 11 **else if** $\dim(I) \neq 0$ **and** $\dim(I)$ is even **and** $\dim([I, I]) \neq 0$
and $\dim([S, S]) = 0$ **then**
/ Case (E) */*
- 12 **find** an $h' \in I$ such that $[h', e] = e$ for all $e \in S$.
- 13 **else if** $\dim(V)$ is even **and** $\dim([S, S]) \neq 0$ **then**
/ Case (F) */*
- 14 **let** h' be a random non-zero element of $[S, S]$
- 15 **end if**,
- 16 **if** h' is defined and $\varphi(h')$ is a split semisimple element of L **then**
- 17 **return** h' .
- 18 **else**
- 19 **return fail**.
- 20 **end if**.

end

Algorithm 10: Finding a split semisimple element in an eigenspace

R	Mult	S	$[S, S]$	$[S, S] \cap H$	I	$[I, I]$	Soln
A_1^{ad}	2	2	0	0	2	2	(C)
A_1^{SC}	2	3	1	1	3	1	(A)
A_3^{SC}	4^3	6	2	2	L	I	(B)
$A_3^{(2)}$	4^3	5	1	1	$L - 1$	I	(A)
B_2^{ad}	2^2	2	0	0	4	0	(C)
\lfloor	4	5	1	1	9	5	(A)
$B_n^{\text{ad}} (n \geq 3)$	2^n	2	0	0	$2n$	0	(C)
\lfloor	$4^{\binom{n}{2}}$	5	1	1	$L - 1$	I	(A)
B_2^{SC}	4	6	2	2	L	6	(D)
\lfloor	4	5	1	1	5	1	(A)
B_3^{SC}	6^3	8	2	2	L	I	(B)
B_4^{SC}	2^4	3	1	1	9	1	(A)
\lfloor	8^3	11	3	3	L	I	(B)
$B_n^{\text{SC}} (n \geq 5)$	2^n	3	1	1	$2n + 1$	1	(A)
\lfloor	$4^{\binom{n}{2}}$	6	2	2	L	I	(B)
$C_n^{\text{ad}} (n \geq 3)$	$2n$	$3n - 1$	$n - 1$	$n - 1$	L		(F)
\lfloor	$2^{n(n-1)}$	3	1	1		I	(A)
$C_n^{\text{SC}} (n \geq 3)$	2n	$3n$	n	n	L		(F)
\lfloor	$4^{\binom{n}{2}}$	5	1	1		I	(A)
D_4^{SC}	8^3	11	3	3	L	I	(B)
$D_4^{(1),(n),(n-1)}$	4^6	5	1	1	$L - 1$	I	(A)
$D_n^{\text{SC}} (n \geq 5)$	$4^{\binom{n}{2}}$	6	2	2	L	I	(B)
$D_n^{(1)} (n \geq 5)$	$4^{\binom{n}{2}}$	5	1	1	$L - 1$	I	(A)
F_4	2^{12}	3	1	1	26	I	(A)
\lfloor	8^3	11	3	3	L	I	(B)
G_2	4^3	5	1	1	L	I	(A)

Table 1: Eigenspaces, their subalgebras, and their ideals in characteristic 2

“ $L - 1$ ” if I is a codimension one ideal of L , and the seventh column contains the dimension of $[I, I]$, or “ I ” if $[I, I] = I$. Finally, the eighth column shows which of the cases of Algorithm 10 is based on this type of root space.

The case distinction in Algorithm 10 is based on the observations in Table 1 in the following manner.

- (A) In each of the cases where $\dim([S, S]) = 1$ we have $[S, S] \subseteq H$, prompting us to take h to be a basis element of $[S, S]$. Note that this case also applies if V corresponds to the direct sum of several Lie algebras of type A_1^{SC} .
- (B) In the cases where $[I, I] = I$ and $\dim([S, S]) \in \{2, 3\}$ we also have $[S, S] \subseteq H$, so that a random non-zero element of $[S, S]$ seems a good candidate.
- (C) In the cases where $\dim([I, I]) = \dim([S, S]) = 0$ the best candidate we can find is an element $h \in M$ that acts on I the way a split semisimple element should. Note that this case also applies if V corresponds to the direct sum of several Lie algebras of type A_1^{ad} .
- (D) In the cases where $\dim(S) = 6$ (prime example being the long roots in B_2^{SC}) we also pick a random non-zero element of $[S, S]$ as candidate.
- (E) This case is special since it does not occur in Table 1. It is however needed to successfully complete the search for a split maximal toral subalgebra if L is of type C_n^{SC} . The solution is similar to that of case (C).
- (F) This case is needed for Lie algebras of type C_n , where again $[S, S] \subseteq H$, but the dimension of $[S, S]$ can be as large as $\dim(H)$. Again, we pick a random non-zero element of $[S, S]$ as candidate.

Given a reductive Lie algebra L , the *reductive rank* of L is the rank of the root datum of L , or, equivalently, the dimension of its split maximal toral subalgebra. In the first line of Algorithm 9 we define d to be $\dim(C_L(\hat{H}))$ for some Cartan subalgebra \hat{H} . This integer is the dimension of H we are aiming for throughout the algorithm, in effect claiming that the reductive rank of L must be d . The validity of this claim is asserted by the following lemma.

Lemma 11. *Let L be a reductive Lie algebra over a field \mathbb{F} whose root datum $R = (X, \Phi, Y, \Phi^\vee)$ is irreducible, and let $d = \text{rk}(R)$ be its reductive rank. If \hat{H} is a (not necessarily split) Cartan subalgebra of L then $\dim(C_L(\hat{H})) = d$.*

Proof By [Hum67, Proposition 15.2] we have that $\hat{H} = C_L(H)$ for some maximal toral subalgebra H of L . Since H is a maximal toral subalgebra, we have $[H, H] = 0$ so that $H \subseteq C_L(H)$. If $H = C_L(H)$, then

$$\dim(C_L(\hat{H})) = \dim(C_L(C_L(H))) = \dim(H) = d,$$

so the only case left to consider is when $H \subsetneq C_L(H)$.

For a suitable field extension, $\mathbb{F}' \supseteq \mathbb{F}$ say, $H_{\mathbb{F}'} = H \otimes \mathbb{F}'$ is split, so $H_{\mathbb{F}'}$ diagonalises $L_{\mathbb{F}'} = L \otimes \mathbb{F}'$ into root spaces L_α . Since we assumed $H \subsetneq C_L(H)$, there exists an L_α such that $[L_\alpha, H_{\mathbb{F}'}] = 0$, so there is a root whose eigenvalue under $H_{\mathbb{F}'}$ is 0. By [CR09, Proposition 3] that means R is of type C_n^{SC} , where $n \geq 2$ (note that this includes B_2^{SC}).

So assume L is of type C_n^{SC} , with $n \geq 2$, with a Chevalley basis $\{X_\alpha \mid \alpha \in \Phi\} \cup \{h_i \mid i = 1, \dots, n\}$, where $h_i \in H$, and let $S = C_L(H)$. Inspection of this family of Lie algebras shows that $\dim(S) = 3n$ and $S = H \cup \langle X_\alpha \mid \alpha \in \Phi^{\text{long}} \rangle$. Moreover, for all $\alpha \in \Phi^{\text{long}}$ we have $[X_\alpha, X_{-\alpha}] \neq 0$ and, as is always the case, $[X_\alpha, X_{-\alpha}] \in H$.

Now suppose $x \in C_L(S)$. Then, since $x \in L$, we have

$$x = \sum_{\alpha \in \Phi} c_\alpha X_\alpha + \sum_{i=1}^n t_i h_i,$$

for some c_α, t_i . If $c_\alpha \neq 0$ for some $\alpha \in \Phi$, then $[x, H] \neq 0$ if α is short, and $[x, X_{-\alpha}] \neq 0$ if α is long (since for all $\beta, \gamma \in \Phi^{\text{long}}$ we have $[X_\beta, H] = 0$, and $[X_\beta, X_\gamma] = 0$ unless $\beta = -\gamma$), in both cases contradicting $[x, S] = 0$. This shows that $x \in H$, and therefore $C_L(S) = H$ and $\dim(C_L(\hat{H})) = \dim(H) = d$, proving the lemma. \square

The lemma immediately generalises to the case where R is not irreducible. We note that a Cartan subalgebra can be computed efficiently [dG00, Section 3.2]. In our experience, in fact, the time it takes to compute a Cartan subalgebra is negligible compared to the overall time taken by Algorithm 9.

We end this section with a number of remarks on the implementation of the algorithm. Firstly, from the manner in which the algorithm is specified we can conclude that it may run for an infinite time. Indeed, M only decreases in dimension if a new split semisimple element is found and such an element does not always exist, as shown in Section 2. Also, in various cases the algorithm `FINDSPLITSEMISIMPLELT` will fail to return a split semisimple h , due to the simple fact that S is not of a suitable type or the candidate h turns out not to be split. In the implementation of this algorithm these problems are remedied by limiting the number of random tries allowed for each M in line 9 of `SPLITMAXIMALTORALSUBALGEBRA` to some finite number. If after that number of tries no new H was found, the algorithm terminates and returns **fail**.

Secondly, note that the influence of the size of the field on the performance of the algorithm is twofold. Firstly, the smaller the field, the higher the probability of finding split semisimple elements in Algorithm 10. On the other hand, the bigger the field, the higher the probability that the random semisimple elements picked in Algorithm 9 have eigenspaces of small dimension. This dichotomy yields an algorithm whose performance is acceptable both over small and over larger fields. We will, of course, in general see a decreasing performance of the algorithm as the size of \mathbb{F} increases, simply because field arithmetic and therefore Lie algebra arithmetic slow down.

6 Implementation and performance

We have implemented the algorithms discussed in the MAGMA computer algebra system [BC10], and comment on the performance of the implementation in this section. We present timings of runs of the `SPLITMAXIMALTORALSUBALGEBRA2` and `SPLITMAXIMALTORALSUBALGEBRA3` algorithms on Lie algebras of split simple algebraic groups over six different fields. In every case the input of the algorithm was the appropriate Chevalley Lie algebra, given as a multiplication table on a uniformly random basis. In Table 2 and in Figure 1, the algorithm was run for Lie algebras up to rank 8, over fields of size 3, 3^6 , and 3^{10} ; in Table 3 and in Figure 3, for Lie algebras up to rank 8, over fields of size 2, 2^6 , and 2^{10} ; and in Figures 2 and 4 for seven different Lie algebras, varying the size of the field between 2 and 2^{40} and between 3 and 3^{40} , respectively. All timings are in seconds and were created using a development version of MAGMA, 2.18, on a 2GHz AMD processor.

We remark that in a sense the timings presented represent the worst possible: because the multiplication table is given on a uniformly random basis it is very dense, making multiplication an exceptionally expensive operation. In practice when a Lie algebra arises from other computations, the multiplication table could be much sparser and the algorithm therefore much faster.

R	GF(3)	GF(3 ⁶)	GF(3 ¹⁰)
A_1^{ad}	0	0	0
A_1^{SC}	0	0	0
A_2^{ad}	0	0	0
A_2^{SC}	0	0	0
A_3^{ad}	0	0	0
$A_3^{(2)}$	0	0	0
A_3^{SC}	0	0	0
A_4^{ad}	0.1	0.1	0.1
A_4^{SC}	0.1	0.1	0.1
A_5^{ad}	0.2	0.5	0.5
$A_5^{(2)}$	0.3	0.5	0.6
$A_5^{(3)}$	0.2	0.4	0.4
A_5^{SC}	0.2	0.4	0.3
A_6^{ad}	0.3	1.1	1.2
A_6^{SC}	0.6	1.1	1.1
A_7^{ad}	1.3	3.3	3.3
$A_7^{(2)}$	1.7	3	4.1
$A_7^{(4)}$	1.2	3.1	4.3
A_7^{SC}	1.7	3.4	4.9
A_8^{ad}	5.2	21	17
$A_8^{(3)}$	5.6	17	21
A_8^{SC}	3	14	10
B_2^{ad}	0	0	0
B_2^{SC}	0	0	0
B_3^{ad}	0	0	0
B_3^{SC}	0	0	0
B_4^{ad}	0.1	0.2	0.3
B_4^{SC}	0.1	0.2	0.3
B_5^{ad}	0.7	1.5	1.8
B_5^{SC}	0.5	1.3	1.4
B_6^{ad}	2.6	8.1	8.2
B_6^{SC}	2.4	6.2	6.9
B_7^{ad}	7.3	23	25
B_7^{SC}	7.9	23	29
B_8^{ad}	37	74	102
B_8^{SC}	25	70	85
C_3^{ad}	0	0	0
C_3^{SC}	0	0	0

R	GF(3)	GF(3 ⁶)	GF(3 ¹⁰)
C_4^{ad}	0.1	0.2	0.3
C_4^{SC}	0.1	0.2	0.3
C_5^{ad}	0.6	1.4	1.7
C_5^{SC}	0.6	1.6	1.5
C_6^{ad}	2.6	7.5	7.9
C_6^{SC}	3	6.5	8
C_7^{ad}	7.3	26	30
C_7^{SC}	7	21	26
C_8^{ad}	29	73	109
C_8^{SC}	22	86	110
D_4^{ad}	0.1	0.1	0.1
$D_4^{(1)}$	0	0.1	0.1
$D_4^{(n-1)}$	0.1	0.1	0.1
$D_4^{(n)}$	0.1	0.1	0.1
D_4^{SC}	0.1	0.2	0.1
D_5^{ad}	0.3	0.8	0.9
$D_5^{(1)}$	0.3	0.7	0.8
D_5^{SC}	0.4	0.6	0.7
D_6^{ad}	1.5	4.9	5
$D_6^{(1)}$	1.3	3.4	3.7
$D_6^{(n-1)}$	1.6	3.9	3.9
$D_6^{(n)}$	1.2	3.7	3.7
D_6^{SC}	1.1	4.6	4.4
D_7^{ad}	3.5	16	19
$D_7^{(1)}$	6	17	17
D_7^{SC}	6.7	19	21
D_8^{ad}	12	54	71
$D_8^{(1)}$	14	48	64
$D_8^{(n-1)}$	10	53	64
$D_8^{(n)}$	12	49	64
D_8^{SC}	12	73	64
E_6^{ad}	3	12	16
E_6^{SC}	2.3	5.9	8
E_7^{ad}	14	66	70
E_7^{SC}	13	88	72
E_8	132	1269	1213
F_4	0.4	0.8	0.8
G_2	0	0	0

Table 2: Runtimes for SPLITMAXIMALTORALSUBALGEBRA3

R	GF(2)	GF(2 ⁶)	GF(2 ¹⁰)
A_1^{ad}	0	0	0
A_1^{SC}	0	0	0
A_2^{ad}	0	0	0
A_2^{SC}	0	0	0
A_3^{ad}	0.1	0.1	0.1
$A_3^{(2)}$	0	0.1	0.1
A_3^{SC}	0	0.1	0.1
A_4^{ad}	0.1	0.4	0.3
A_4^{SC}	0.1	0.4	0.3
A_5^{ad}	0.4	1.8	1.2
$A_5^{(2)}$	0.4	2.2	1.7
$A_5^{(3)}$	0.4	1.8	1.2
A_5^{SC}	0.4	2.3	1.6
A_6^{ad}	1.1	6.2	4.9
A_6^{SC}	1	6.2	4.1
A_7^{ad}	4.3	18	13
$A_7^{(2)}$	4.3	20	17
$A_7^{(4)}$	3.4	20	16
A_7^{SC}	3.8	22	14
A_8^{ad}	9.9	51	35
$A_8^{(3)}$	9.8	46	43
A_8^{SC}	9.6	50	37
B_2^{ad}	0	0	0
B_2^{SC}	0	0.1	0.1
B_3^{ad}	0.1	0.2	0.2
B_3^{SC}	0.1	0.3	0.3
B_4^{ad}	0.3	1.6	1.4
B_4^{SC}	0.4	2.4	1.9
B_5^{ad}	1.6	8.9	7.3
B_5^{SC}	1.7	10	7.1
B_6^{ad}	6	38	31
B_6^{SC}	8.1	45	28
B_7^{ad}	20	121	89
B_7^{SC}	22	128	114
B_8^{ad}	70	353	319
B_8^{SC}	77	405	311
C_3^{ad}	0.1	0.4	0.3
C_3^{SC}	0.1	0.4	0.3

R	GF(2)	GF(2 ⁶)	GF(2 ¹⁰)
C_4^{ad}	0.8	2.4	1.7
C_4^{SC}	0.3	2	1.8
C_5^{ad}	4.7	20	8.1
C_5^{SC}	1.6	12	8.5
C_6^{ad}	35	111	50
C_6^{SC}	6.7	43	41
C_7^{ad}	97	244	218
C_7^{SC}	21	156	129
C_8^{ad}	375	1059	1099
C_8^{SC}	67	510	472
D_4^{ad}	0.4	0.8	0.5
$D_4^{(1)}$	0.3	0.8	0.8
$D_4^{(n-1)}$	0.1	0.8	0.7
$D_4^{(n)}$	0.2	0.9	0.7
D_4^{SC}	0.2	1.1	0.8
D_5^{ad}	0.9	4.2	3.3
$D_5^{(1)}$	0.8	5.2	3.6
D_5^{SC}	0.9	4.6	4.1
D_6^{ad}	5.8	20	16
$D_6^{(1)}$	4	22	14
$D_6^{(n-1)}$	6.4	24	15
$D_6^{(n)}$	5.4	23	15
D_6^{SC}	5.3	25	20
D_7^{ad}	24	98	53
$D_7^{(1)}$	14	79	53
D_7^{SC}	12	78	62
D_8^{ad}	57	293	166
$D_8^{(1)}$	55	218	184
$D_8^{(n-1)}$	120	266	224
$D_8^{(n)}$	66	322	162
D_8^{SC}	54	314	228
E_6^{ad}	5.7	33	31
E_6^{SC}	5.2	33	31
E_7^{ad}	65	268	258
E_7^{SC}	72	300	217
E_8	492	4261	3795
F_4	1.5	8.2	5.6
G_2	0	0.1	0

Table 3: Runtimes for SPLITMAXIMALTORALSUBALGEBRA2

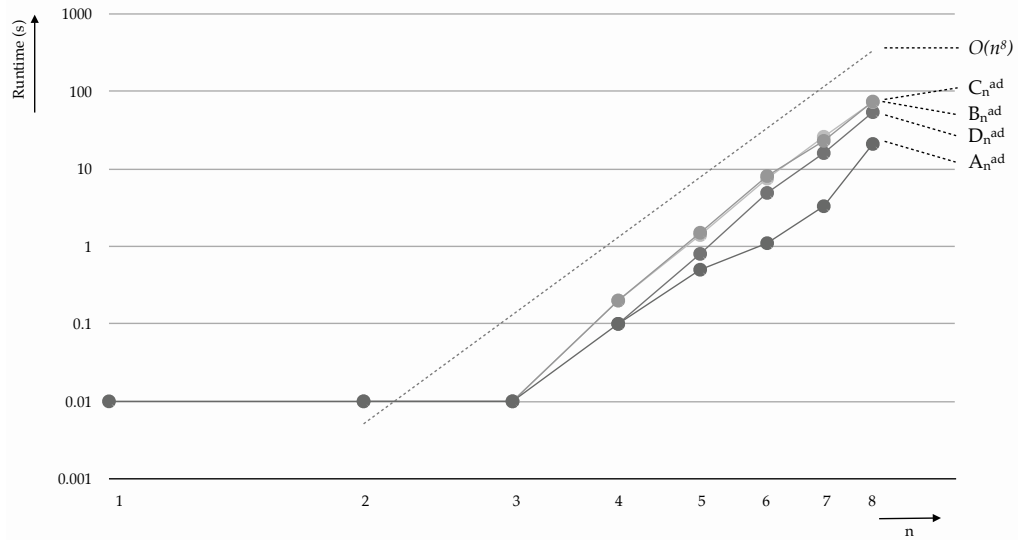


Figure 1: Runtimes for SPLITMAXIMALTORALSUBALGEBRA3 for $\mathbb{F} = \text{GF}(3^6)$

Despite the fact that we have not commented on the computational complexity of our algorithm, the four graphs give some indication. In particular, Figures 1 and 3 suggest a dependence on the rank n of approximately $O(n^8)$ and Figures 2 and 4 suggest a linear dependence on the logarithm of the size of the field. This leads to an approximate complexity of $O(n^8 \log(q))$, where n is the reductive rank of the Lie algebra and q the size of the field. This is not as bad as it may seem at first sight, as a single Lie multiplication already takes $O(n^6 \log(q))$ time.

Acknowledgements

The author would like to thank Arjeh Cohen for numerous fruitful discussions on this topic and the anonymous reviewers for their thorough evaluation and their valuable comments.

References

- [BC10] W. Bosma and J. J. Cannon, editors. *Handbook of Magma Functions, Edition 2.17*. School of Mathematics and Statistics, University of Sydney, 2010. <http://magma.maths.usyd.edu.au/>.
- [Bor91] Armand Borel. *Linear Algebraic Groups*. Springer-Verlag, New York, second edition, 1991.
- [Car72] Roger W. Carter. *Simple groups of Lie type*. Pure and Applied Mathematics (New York). John Wiley & Sons Inc., New York, 1972.
- [Che58] C. Chevalley. *Classification des groupes de Lie algébriques*. Séminaire Ecole Normale Supérieure, Paris, 1956–1958.

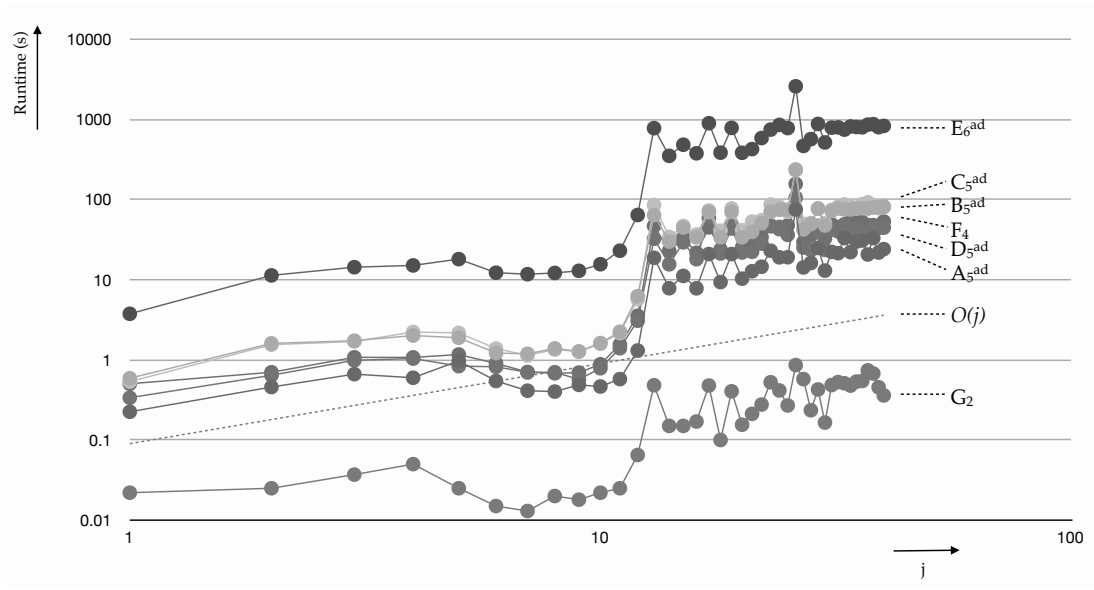


Figure 2: Runtimes for SPLITMAXIMALTORALSUBALGEBRA3 for $\mathbb{F} = \text{GF}(3^j)$, $1 \leq j \leq 40$

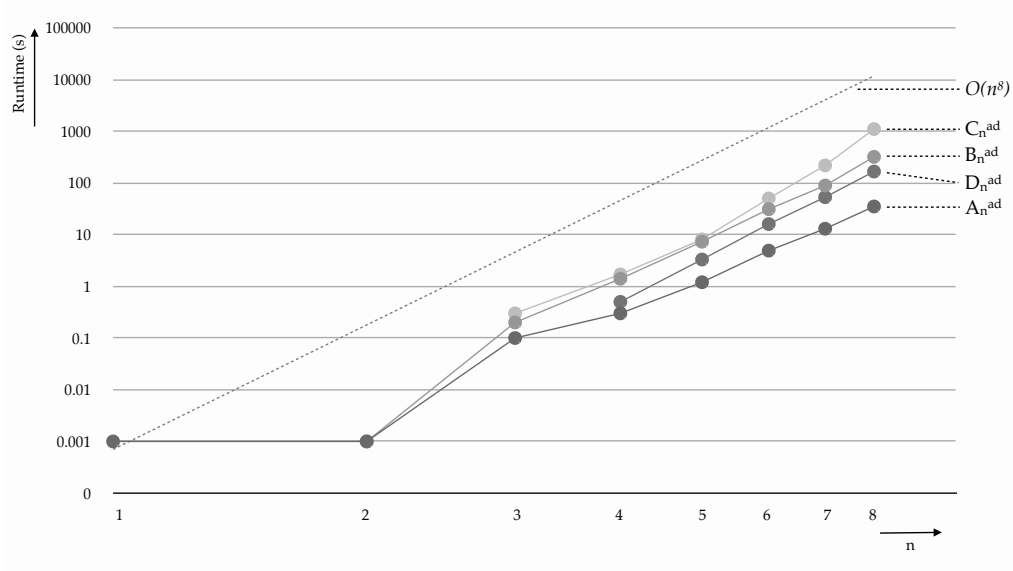


Figure 3: Runtimes for SPLITMAXIMALTORALSUBALGEBRA2 for $\mathbb{F} = \text{GF}(2^6)$

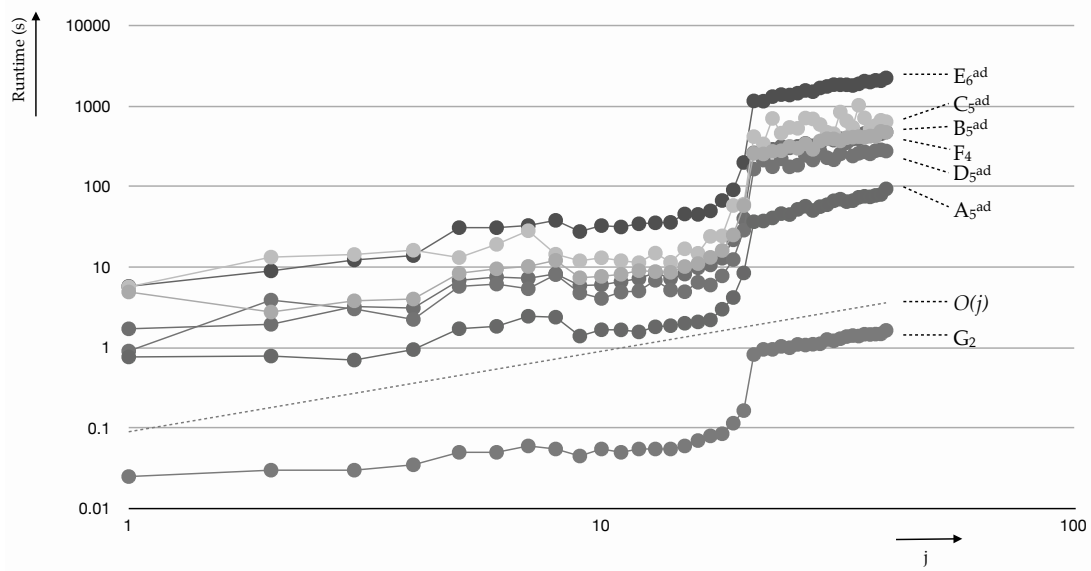


Figure 4: Runtimes for SPLITMAXIMALTORALSUBALGEBRA2 for $\mathbb{F} = \text{GF}(2^j)$, $1 \leq j \leq 40$

- [CM09] Arjeh M. Cohen and Scott H. Murray. An algorithm for Lang's theorem. *Journal of Algebra*, 322:675–702, 2009.
- [CR09] Arjeh M. Cohen and Dan Roozemon. Computing Chevalley bases in small characteristics. *J. Algebra*, 322(3):703–721, August 2009.
- [dG00] Willem A. de Graaf. *Lie Algebras: Theory and Algorithms*, volume 56 of *North Holland Mathematical Library*. Elsevier Science, 2000.
- [Hum67] James E. Humphreys. *Algebraic groups and modular Lie algebras*, volume 71 of *Memoirs of the American Mathematical Society*. American Mathematical Society, Providence, Rhode Island, 1967.
- [Hum75] James E. Humphreys. *Linear Algebraic Groups*. Graduate Texts in Mathematics. Springer-Verlag New York, 1975.
- [Roo10] D.A. Roozemon. *Algorithms for Lie algebras of algebraic groups*. PhD thesis, Technische Universiteit Eindhoven, 2010.
- [Ryb07] Alexander J. E. Ryba. Computer construction of split Cartan subalgebras. *J. Algebra*, 309(2):455–483, 2007.
- [Spr98] T.A. Springer. *Linear Algebraic Groups*, volume 9 of *Progress in Mathematics (Boston, Mass.)*. Birkhäuser, second edition, 1998.